Advanced Information Security for Technical Staff

Dates

2005 Dates

February 28-March 4, 2005 (SEI Pittsburgh, PA)
May 23-27, 2005 (SEI Pittsburgh, PA)
August 29-September 2, 2005 (SEI Pittsburgh, PA)
October 24-28, 2005 (SEI Pittsburgh, PA)

This course may also be offered by arrangement at customer sites. E-mail course-info@sei.cmu.edu or call +1 412-268-7622 for details.

Prices (USD)

U.S.

Industry: $2625
Government: $2100
Academic: $2100

International

$5250

2005

REGISTER

Course Registration
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-7388
FAX: 412 / 268-7401
E-mail: courseregistration@sei.cmu.edu

Course Description

This five-day course is designed to increase the depth of knowledge and skills of technical staff charged with administering and securing information systems and networks. Developed around a scenario in which a production network has failed an information security audit, students will implement numerous technical security solutions to bring the network into compliance. Participants will work in teams to integrate these solutions throughout the enterprise. Each student will have the use of a dual-boot laptop for the duration of the course, as well as direct administrative access to a wide variety of networked systems.

The first two days of the course will cover host system hardening, system availability monitoring, network access control and applied encryption technologies, intrusion detection systems, as well as logging, forensics, and incident analysis and response techniques. Instructors will utilize lecture/presentations, demonstrations and hands-on exercises to teach these topic areas.

During the final 3 days, instructors will facilitate participants through the implementation of the network's get-well plan and compliance task list. Students will use various freeware/open-source software and operating system specific technologies to accomplish these tasks. Following are some examples of the required tasks:

- implement a new segmented network topology and IP addressing scheme

- install, configure and test 2 enterprise class, Unix-based firewalls and create a DMZ to isolate public services
- implement an isolated administrative/management network
- install, configure an email forwarder and spam-filtering server
- install, configure a centralized syslog server and configure hosts to send encrypted log information to this system
- install, configure network-time synchronization services
- implement Split-DNS name resolution services
- install, configure and test IPSEC VPN termination points and implement secure remote access
- install, configure an HTTP application proxy server and implement content filtering
- install, configure several intrusion detection sensors to include Snort/ACID
- utilize Windows 2000 group policy, security templates, and numerous other technologies and techniques to harden Windows hosts
- utilize Bastille, Tripwire, and numerous other technologies and techniques to harden Linux systems
- install, configure system availability monitoring tools and configure alerts Configure numerous network monitoring stations and analyze data for suspicious events
- inspect and systematically analyze log and IDS data for malicious activity

Audience · Prerequisites · Objectives · Logistics

AUDIENCE

Technical staff members who manage or support networked information systems and have

- two years of practical experience with networked systems or equivalent training/education
- six months of security administration experience
- strong background in data networking with some specific degree of Unix or Windows system administration experience

PREREQUISITES

Before registering for this course, participants must complete the Information Security for Technical Staff course or have equivalent training or experience.

TOPICS

- Windows and Unix host system hardening
- system availability monitoring
- network access control techniques and applied encryption
- secure network architectures and topologies
- intrusion detection systems
- secure implementation of logging and network monitoring
- forensic analysis and incident response

OBJECTIVES

- evaluate and integrate information security technologies
- install/configure network access control technologies
- install/configure intrusion detection sensors
- implement technology to ensure confidentially of network traffic
- implement techniques for hardening host systems and services
- implement technology for monitoring the status/availability of network services
- implement system logging and network monitoring

- analyze and respond to network and system events

LOGISTICS

Class Schedule

This five-day course meets at the following times:
Days 1-4, 9:00 a.m.-5:00 p.m.
Day 5, 9:00 a.m.-2:30 p.m.

Hotel and Travel Information

Information about traveling to SEI offices in Pittsburgh, Pennsylvania and Arlington, Virginia is available on our Travel and Lodging Web pages.

Questions about this course?

Please see our Frequently Asked Questions Web page for answers to some of the more common inquiries about SEI Education and Training. If you need more information, contact us via e-mail at course-info@sei.cmu.edu or telephone at +1 412-268-7622.

Related Products and Services

Courses

Information Security for Technical Staff
Information Security for Network Managers

Other Related Information

CERT Web site

Related Information

CERT-Certified Incident Handler Certification
CERT Training and Education

Course Registration

2005

^
TOP

URL: http://www.sei.cmu.edu/products/courses/cert/adv-infosec-tech.html
Last Modified: 20 April 2005